

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

PR9



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/761,742	01/08/2001	Makoto Kayashima	566.39530X00	6168
20457	7590	07/15/2004		EXAMINER
ANTONELLI, TERRY, STOUT & KRAUS, LLP 1300 NORTH SEVENTEENTH STREET SUITE 1800 ARLINGTON, VA 22209-9889				ZIA, SYED
			ART UNIT	PAPER NUMBER
			2131	

DATE MAILED: 07/15/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/761,742	KAYASHIMA ET AL.
Examiner	Art Unit	
Syed Zia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM
 THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 18 January 2001.
 2a) This action is **FINAL**. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-7 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1-7 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) Notice of References Cited (PTO-892)
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
 Paper No(s)/Mail Date _____.
- 4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date. _____.
 5) Notice of Informal Patent Application (PTO-152)
 6) Other: _____.

DETAILED ACTION

This office action is in response to preliminary amendment filed on May 18, 2001.

Original application contained Claims 1-13. Applicant cancelled Claims 8-13. Therefore, Claims 1-7 are pending for consideration and examination.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-7 are rejected under 35 U.S.C. 102(e) as being anticipated by Wiegel (U. S. Patent 6,484,261).

2. Regarding Claim 1 Wiegel teaches and describes a security management system for controlling a security status of each of a plurality of managed systems constituting an

information system in accordance with an information security policy representing a policy of a security measure (Fig.1-4), comprising:

a plurality of management sections corresponding to at least one managed system and the information security policy, each management section being for controlling the security status of the managed system corresponding thereto so as to adjust the security status to the information security policy corresponding thereto (col.7 line 12 to col.8 line 26);

a database registering a correspondence of the information security policy, the managed system and each management section (col.14 line 4 to line 61);

a security content reception section for receiving a selection of a range of the information security policy and the managed system from a user, and an extraction section for extracting from said database the management section registered so as to correspond to the information security policy and the managed system included in the range in which said security content reception section has received the selection (col.8 line 66 to col.10 line 41); and

a management control section for allowing the management section extracted by said extraction section to change the security status of the managed system corresponding to the management section so as to adjust to the information security policy corresponding to the management section (col.14 line 62 to col.16 line 34).

3. Regarding Claim 2 Wiegel teaches and describes security a management system for auditing a security status of each of a plurality of managed systems constituting an information system, the security status concerning an information security policy representing a policy of a security measure (Fig.1-4), comprising:

a plurality of audit sections corresponding to at least one managed system and at least one information security policy, each audit section being for auditing the security status concerning the corresponding information security policy of the corresponding managed system (col.7 line 12 to col.8 line 26);

a database registering a correspondence of the information security policy, the managed system and the audit section (col.14 line 4 to line 61);

a security content reception section for receiving a selection of a range of the information security policy and the managed system from the user, and an extraction section for extracting from said database the audit section registered so as to correspond to the information security policy and the managed system included in the range in which said security content reception section has received the selection (col.8 line 66 to col.10 line 41, and col.14 line 62 to col.16 line 34); and

an audit control section for allowing the audit section extracted by said extraction section to audit the security status concerning the information security policy of the managed system corresponding to the audit section (col.12 line 61 to col.13 line 67).

4. Regarding Claim 3 Wiegel teaches and describes a security management system for controlling a security status of each of a plurality of managed systems constituting an information system in 4 accordance with an information security policy representing a policy of a security measure (Fig.1-4), comprising:

a plurality of management sections corresponding to at least one managed system and at least one information security policy, each management section being for controlling the security

status of the corresponding managed system so as to adjust the security state to the corresponding information security policy, and a plurality of audit sections corresponding to at least one managed system and at least one information security policy, each audit section being for auditing the security status concerning the corresponding information security policy of the corresponding managed system (col.7 line 12 to col.8 line 26);

a database registering a correspondence of the information security policy, the managed system, the management section and the audit section (col.14 line 4 to line 61);

a security content reception section for receiving a selection of a range of the information security policy and the managed system from a user, and an extraction section for extracting from said database the management section and the audit section, which are registered so as to correspond to the information security policy and the managed system included in the range in which said security content reception section has received the selection (col.8 line 66 to col.10 line 41);

-a management control section for allowing the management section extracted by said extraction section to change the security status of the managed system corresponding to the management section so as to adjust to the information security policy corresponding to the management section (col.14 line 62 to col.16 line 34); and

an audit control section for allowing the audit section extracted by said extraction section to audit the security status concerning the information security policy of the managed system corresponding to said audit section (col.12 line 61 to col.13 line 67).

5. Regarding Claim 4 Wiegel teaches and describes a security management method for controlling a security status of each of a plurality of managed systems constituting an information system with an electronic computer in accordance with an information security policy representing a policy of a security measure (Fig.1-4), comprising the steps of: receiving a selection of a range of the information security policy and the managed system from a user, and extracting a management program corresponding to an information security policy and a managed system, included in the range in which the selection has been received, among a plurality of management programs describing a processing for controlling the security status of the corresponding managed system so as to adjust the security status to the corresponding information security policy, the plurality of management programs corresponding to at least one information security policy and at least one managed system, which are previously stored (col.7 line 12 to col.8 line 26, and col.8 line 66 to col.10 line 41, and col.14 line 62 to col.16 line 34); and

allowing the electronic computer to execute the extracted management program and to change the security status of the managed system corresponding to the management program so that the security status thereof is adjusted to the information security policy corresponding to the management program (col.14 line 62 to col.16 line 34, and col.12 line 61 to col.13 line 67).

6. Regarding Claim 5 Wiegel teaches and describes a security management method for auditing, with an electronic computer, a security status of each of a plurality of managed systems constituting an information system, the security status concerning an information security policy representing a policy of a security measure (Fig.1-4), comprising the steps of:

receiving a range of a selection of the information security policy and the managed system from a user, and extracting an audit program registered so as to correspond to the information security policy and the managed system, which are included in the range in which the selection has been received, among a plurality of audit programs describing a processing for auditing the security status concerning the corresponding information security policy of the corresponding managed system, the plurality of audit programs corresponding to at least one information security policy and at least one managed system, which are previously stored (col.7 line 12 to col.8 line 26, and col.8 line 66 to col.10 line 41, and col.14 line 62 to col.16 line 34); and

allowing the electronic computer to execute the extracted audit program and to audit the security status of the managed system corresponding to the audit program the security status concerning the information security policy corresponding to the audit program (col.14 line 62 to col.16 line 34, and col.12 line 61 to col.13 line 67).

7. Regarding Claim 6 Wiegel teaches and describes storage medium storing a program for controlling a security status of each of a plurality of managed systems constituting an information system in accordance with an information security policy representing a policy of a security measure, wherein said program is read out and executed by an electronic computer, to construct, on said electronic computer, a security content reception section for receiving a selection of a range of the information security policy and the managed system from a user (Fig.1-4, and col.10 line 44 to col.12line 2);

an extraction section for extracting a management program corresponding to an information security policy and a managed system, which are included in the range in which said

security content reception section has received the selection, from a database storing a plurality of management programs describing a processing for controlling the security status of the corresponding managed system so as to adjust the security status of the managed system to the corresponding information security policy, the plurality of management programs corresponding at least one managed system and at least one information security policy (col.7 line 12 to col.8 line 26, and col.8 line 66 to col.10 line 41, and col.14 line 62 to col.16 line 34); and a management control section for allowing said electronic computer to execute the management program executed by said extraction section and to change the security status of the managed system corresponding to the extracted management program so as to adjust the security status to the information security policy corresponding to the extracted management program (col.14 line 62 to col.16 line 34, and col.12 line 61 to col.13 line 67).

8. Regarding Claim 7 Wiegel teaches and describes a storage medium storing a program for auditing a security status concerning an information security policy representing a policy of a security measure of a plurality of managed systems constituting an information system (Fig.1-4, col.10 line 44 to col.12line 2), wherein

 said program is read out and executed by an electronic computer, to construct, on said electronic computer, a security content reception section for receiving a selection of a range of the information security policy and the managed system from a user; an extraction section for extracting an audit program registered so as to correspond to an information security policy and a managed system, which are included in the range in which said security content reception section has received the selection, from a database storing a plurality of audit programs describing a

processing for auditing the security status concerning the corresponding information security policy of the corresponding managed system, the plurality of audit programs corresponding to at least one managed system and at least one information security policy (col.7 line 12 to col.8 line 26, col.8 line 66 to col.10 line 41, and col.14 line 62 to col.16 line 34); and

an audit control section for allowing the electronic computer to execute the audit program extracted by said extraction section and to audit the security status concerning the Information security policy corresponding to the audit program of the managed system corresponding to the audit program (col.14 line 62 to col.16 line 34, and col.12 line 61 to col.13 line 67).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Syed Zia whose telephone number is 703-305-3881. The examiner can normally be reached on Monday - Friday 9:00 AM to 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SZ
July 07, 2004


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100